AMENDMENTS TO CLAIMS

Claim 1 (original): A system for secure transmission of protected content, the system comprising:

a security server;

a recipient module; and

a secure communication channel for supporting communication between said security server and said recipient module,

wherein, in a first mode of operation, the recipient module receives a first key in a multiple key hierarchy via said secure channel, and

in a second mode of operation, the recipient module receives the protected content and an encrypted key, said encrypted key being a second key in said multiple key hierarchy, said recipient module being operative to utilize the first key to decrypt the encrypted key to form a decrypted key, said recipient module only being capable of accessing the protected content with said decrypted key.

Claim 2 (original): The system of claim 1, wherein said first key is contained in a VEMM, said VEMM further comprising an access criteria reference for determining whether said recipient module is entitled to access the protected content and said VEMM being prepared by said security server.

Claim 3 (original): The system of claim 2, wherein said access criteria reference for each item of protected content is associated with a separate access key.

Claim 4 (original): The system of claim 2, wherein said encrypted key further comprises an encrypted control word.

Claim 5 (original): The system of claim 4, wherein said encrypted control word is contained in a VECM, said VECM further comprising an access criteria reference for identifying said first key for decrypting said encrypted control word by said recipient module and said VECM being prepared by said security server.

Claim 6 (original): The system of claim 5, wherein said secure communication channel further comprises a subscriber key, such that said first key is encrypted with said subscriber key for being transmitted to said recipient module, and such that said recipient module is capable of decrypting said subscriber key.

Claim 7 (original): The system of claim 6, wherein said recipient module further comprises a secret, said secret being required for decrypting said subscriber key, and said secret comprising a part of said secure communication channel.

Claim 8 (original): The system of claim 7, wherein said recipient module comprises at least one permanent read-only storage medium for storing said secret.

Claim 9 (original): The system of claim 8, wherein said secret is permanently stored on said at least one permanent read-only storage medium during manufacture of said recipient module.

Claim 10 (original): The system of claim 9, wherein said recipient module comprises at least one generic chip, said at least one generic chip comprising said at least one permanent read-only storage medium for storing said secret.

Claim 11 (original): The system of claim 7, wherein said security server receives said subscriber key encrypted with said secret and an unencrypted subscriber key, but wherein said security server does not receive said secret.

Claim 12 (original): The system of claim 7, further comprising a head-end for transmitting the protected content.

Claim 13 (original): The system of claim 12, wherein said head-end sends a EMM to said security server, for providing said access criteria reference to said security server.

Claim 14 (original): The system of claim 13, wherein said head-end sends at least information for generating said control word to said security server in an ECM.

Claim 15 (original): The system of claim 14, wherein said head-end also sends said ECM to said recipient module.

Claim 16 (original): The system of claim 14, wherein a different VEMM is transmitted periodically.

Claim 17 (original): The system of claim 16, wherein a different VEMM is transmitted if said recipient module is off-line for at least a predetermined period of time.

Claim 18 (original): The system of claim 14, further comprising a plurality of recipient modules, wherein said VEMM is unicast to each of a subset of said plurality of recipient modules.

Claim 19 (original): The system of claim 14, further comprising a remote renewable security element for storing said subscriber key and for providing said encrypted first key and said encrypted control word to said security server.

Claim 20 (original): The system of claim 19, wherein said subscriber key at said remote renewable security element is capable of being renewed.

Claim 21 (original): The system of claim 19, wherein said remote renewable security element further comprises a hardware component and a software component.

Claim 22 (original): The system of claim 21, wherein said software component determines one or more entitlements for permitting said VEMM to be generated for said recipient module.

Claim 23 (original): The system of claim 21, wherein said hardware component encrypts said access key and said control word.

Claim 24 (original): The system of claim 19, further comprising a plurality of said remote renewable security elements, and further comprising a broadcaster of the protected content for controlling said plurality of said remote renewable security elements.

Claim 25 (original): The system of claim 19, wherein a plurality of said remote renewable security elements is controlled by said security server.

Claim 26 (original): The system of claim 25, wherein said security server and said plurality of said remote renewable security elements share a server key for at least decrypting at least said access key.

Claim 27 (original): The system of claim 26, wherein said security server generates said access key in an encrypted form as an encrypted access key, and wherein said remote renewable security element decrypts said encrypted access key to form said access key according to said server key.

Claim 28 (original): The system of claim 19, wherein said recipient module comprises a set-top box.

Claim 29 (original): A system for secure transmission of protected content, comprising:

(a) a remote renewable security element for encrypting a plurality of keys in a multiple key hierarchy; and

(b) a recipient module for receiving the protected content and said plurality of encrypted keys, said recipient module comprising a secret for decrypting at least one encrypted key to form a first decrypted key, said first decrypted key being required to decrypt at least one additional key in said multiple key hierarchy, wherein said recipient module is only capable of accessing the

protected content with said at least one additional decrypted key in said multiple key hierarchy.

Claim 30 (original): The system of claim 29, wherein said first encrypted key is only capable of being decrypted according to said secret.

Claim 31 (original): The system of claim 30, wherein said recipient module comprises at least one permanent read-only storage medium for storing said secret.

Claim 32 (original): The system of claim 31, wherein said secret is permanently stored on said at least one permanent read-only storage medium during manufacture of said recipient module.

Claim 33 (original): The system of claim 32, wherein said recipient module comprises at least one generic chip, said at least one generic chip comprising said at least one permanent read-only storage medium for storing said secret.

Claim 34 (original): The system of claim 33, comprising a plurality of said remote renewable security elements, and further comprising a broadcaster of the protected content for controlling said plurality of said remote renewable security elements.

Claim 35 (original): The system of claim 29, wherein at least one of said keys in said multiple key hierarchy at said remote renewable security element is capable of being renewed.

Claim 36 (original): The system of claim 29, wherein said remote renewable security element comprises at least one encryption mechanism.

Claim 37 (original): The system of claim 36, further comprising a security server for receiving said first encrypted key encrypted with said secret and also for receiving said first key as an unencrypted key, such that said secret is not accessible to said security server or to said remote renewable security element.

Claim 38 (original): The system of claim 37, further comprising a head-end for broadcasting the protected content.

Claim 39 (original): The system of claim 38, wherein said head-end transmits an access criteria reference to said security server, and wherein said security server packages said access criteria reference at least with said first encrypted key for transmitting to said recipient module.

Claim 40 (original): The system of claim 39, wherein said head-end sends a EMM to said security server, for providing said access criteria reference to said security server.

Claim 41 (original): The system of claim 40, wherein said security server constructs a VEMM from said EMM and sends said VEMM to said recipient module.

Claim 42 (original): The system of claim 41, wherein a different VEMM is transmitted periodically.

Claim 43 (original): The system of claim 41, wherein said security server receives an access key, encrypted with said first key, from said remote renewable security element, and wherein said security server sends said encrypted access key to said recipient module.

Claim 44 (original): The system of claim 43, wherein said access key is not sufficient to access the protected content, and wherein said security server receives a control word, encrypted with said access key, from said remote renewable security element, and wherein said security server sends said encrypted control word to said recipient module, said control word being sufficient for said recipient module to access the protected content.

Claim 45 (original): The system of claim 44, wherein said security server receives said control word from said head-end.

Claim 46 (original): The system of claim 44, wherein said head-end sends at least information for generating said control word to said security server in an ECM.

Claim 47 (original): The system of claim 46, wherein said head-end also sends said ECM to said recipient module.

Claim 48 (original): The system of claim 47, further comprising a set-top box for receiving the protected content, said set-top box comprising a smart card located at said set-top box, said set-top box receiving said ECM and said EMM from said head-end if said set-top box is authorized to access the protected content, such that said set-top box is not required to be in communication with said security server.

Claim 49 (original): The system of claim 39, wherein said recipient module comprises a set-top box.

Claim 50 (original): The system of claim 49, wherein each access criteria reference is associated with a different access key.

Claims 51 - 62 (cancelled)

Claim 63 (withdrawn): The system of claim 2 and wherein said VEMM is sent upon request by said recipient module.

Claim 64 (withdrawn): The system of claim 63 and wherein said request includes an access criteria reference.

Claim 65 (withdrawn): The system of claim 63 and wherein said request is initiated in response to an impulse pay per view (IPPV) request by a user.

Claim 66 (withdrawn): The system of claim 5 and wherein said secure communication channel further comprises a subscriber key, such that said first key is encrypted with said subscriber key for being transmitted to said recipient module, and such that only said recipient module is capable of decrypting said subscriber key.

Claim 67 (withdrawn): The system of claim 1 and wherein at least one of said security server and said secure communication channel is implemented with redundant components.

Claim 68 (withdrawn): The system of claim 41 and wherein said VEMM is sent upon request by said recipient module.

Claim 69 (withdrawn): The system of claim 68 and wherein said request includes an access criteria reference.

Claim 70 (withdrawn): The system of claim 68 and wherein said request is initiated in response to an impulse pay per view (IPPV) request by a user.

Claim 71 (withdrawn): The system of claim 29 and wherein said remote renewable security element is implemented with redundant components.

Claims 72 - 82 (cancelled)

Claim 83 (new): A system for secure transmission of protected content, the system comprising:

a head-end operative to send entitlement information controlling access to the protected content;

a security server;

a plurality of recipient modules; and

a secure communication channel for supporting communication between said security server and at least one of said plurality of recipient modules, wherein

the head-end sends the entitlement information both to the security server and to at least some of the plurality of recipient modules; and

said plurality of recipient modules comprises:

a first plurality of security-element recipient modules; and

a second plurality of non-security-element recipient modules, the first plurality of recipient modules differing from said second plurality of recipient modules in that each of the first plurality of security-element recipient modules includes a renewable security element operative to process the entitlement information received from the head-end and produce therefrom a key for accessing the protected content, and

in a first mode of operation, at least one of the non-security-element recipient modules receives a first key in a multiple key hierarchy via said secure communication channel, and

in a second mode of operation, said at least one of the non-security-element recipient modules receives the protected content and an encrypted key, said encrypted key being a second key in said multiple key hierarchy, said at least one of the non-security-element recipient modules being operative to utilize the first key to decrypt the encrypted key to form a decrypted key, said at least one of the non-security-element recipient modules only being capable of accessing the protected content with said decrypted key, and

said first key and said second key are prepared by said security server based, at least in part, on the entitlement information sent by the head-end.

Claim 84 (new): The system according to claim 83, wherein said first key is contained in a VEMM, said VEMM further comprising an access criteria reference for determining whether said at least one of the non-security-element recipient modules is entitled to access the protected content, said VEMM being prepared by said security server based, at least in part, on the entitlement information sent by the head-end.

Claim 85 (new): The system according to claim 84 and wherein said VEMM is sent upon request by said at least one of the non-security-element recipient modules.

Claim 86 (new): The system according to claim 85 and wherein said request includes an access criteria reference.

Claim 87 (new): The system according to claim 85 and wherein said request is initiated in response to an impulse pay per view (IPPV) request by a user.

Claim 88 (new): The system according to claim 84, wherein said access criteria reference for each item of protected content is associated with a separate access key.

Claim 89 (new): The system according to claim 84, wherein said encrypted key further comprises an encrypted control word.

Claim 90 (new): The system according to claim 89, wherein said encrypted control word is contained in a VECM, said VECM further comprising an access criteria reference for identifying said first key for decrypting said encrypted control word by said at least one of the non-security-element recipient modules, said VECM being prepared by said security server based, at least in part, on the entitlement information sent by the head-end.

Claim 91 (new): The system according to claim 90, wherein said secure communication channel further comprises a subscriber key, such that said first key is encrypted with said subscriber key for being transmitted to said at least one of the non-security-element recipient modules, and such that said at least one of the non-security-element recipient modules is capable of decrypting said subscriber key.

Claim 92 (new): The system according to claim 90, wherein said secure communication channel comprises a second plurality of secure communication channels each associated with one of the second plurality of non-security-element recipient modules, and

each of the secure communication channels further comprises a subscriber key of the associated one of the non-security-element recipient modules, such that said first key is encrypted with said subscriber key for being transmitted to said one of the non-security-element recipient modules, and such that only said one of the non-security-element recipient modules is capable of decrypting said subscriber key.

Claim 93 (new): The system according to claim 91, wherein said one of the non-security-element recipient modules further comprises a secret, said secret being required for decrypting said subscriber key, and said secret comprising a part of said secure communication channel.

Claim 94 (new): The system according to claim 93, wherein said one of the non-security-element recipient modules comprises at least one permanent read-only storage medium for storing said secret.

Claim 95 (new): The system according to claim 94, wherein said secret is permanently stored on said at least one permanent read-only storage medium during manufacture of said one of the non-security-element recipient modules.

Claim 96 (new): The system according to claim 94, wherein said one of the non-security-element recipient modules comprises at least one generic chip, said at least one generic chip comprising said at least one permanent read-only storage medium for storing said secret.

Claim 97 (new): The system according to claim 93, wherein said security server receives said subscriber key encrypted with said secret and an unencrypted subscriber key, but wherein said security server does not receive said secret.

Claim 98 (new): The system according to claim 84, wherein said head-end sends a EMM to said security server, for providing said access criteria reference to said security server.

Claim 99 (new): The system according to claim 98, wherein said head-end sends at least information for generating said control word to said security server in an ECM.

Claim 100 (new): The system according to claim 99, wherein said head-end also sends said ECM to at least one of the security-element recipient modules.

Claim 101 (new): The system according to claim 99, wherein a different VEMM is transmitted periodically.

Claim 102 (new): The system according to claim 101, wherein a different VEMM is transmitted if said at least one of the non-security-element recipient modules is off-line for at least a predetermined period of time.

Claim 103 (new): The system according to claim 99, wherein said VEMM is unicast to each of a subset of said plurality of recipient modules.

Claim 104 (new): The system according to claim 99, wherein said security server comprises a remote renewable security element for storing said subscriber key and for providing said encrypted first key and said encrypted control word to said security server.

Claim 105 (new): The system according to claim 104, wherein said subscriber key at said remote renewable security element is capable of being renewed.

Claim 106 (new): The system according to claim 104, wherein said remote renewable security element further comprises a hardware component and a software component.

Claim 107 (new): The system according to claim 106, wherein said software component determines one or more entitlements for permitting said VEMM to be generated for said at least one of the non-security-element recipient modules.

Claim 108 (new): The system according to claim 106, wherein said hardware component encrypts said access key and said control word.

Claim 109 (new): The system according to claim 104, further comprising a plurality of said remote renewable security elements, and further comprising a broadcaster of the protected content for controlling said plurality of said remote renewable security elements.

Claim 110 (new): The system according to claim 104, wherein a plurality of said remote renewable security elements is controlled by said security server.

Claim 111 (new): The system according to claim 110, wherein said security server and said plurality of said remote renewable security elements share a server key for at least decrypting at least said access key.

Claim 112 (new): The system according to claim 111, wherein said security server generates said access key in an encrypted form as an encrypted access key, and wherein said remote renewable security element decrypts said encrypted access key to form said access key according to said server key.

Claim 113 (new): The system according to claim 104, wherein at least some of said plurality of recipient modules each comprise a set-top box.

Claim 114 (new): The system according to claim 83 and wherein at least one of said security server and said secure communication channel is implemented with redundant components.

Claim 115 (new): The system according to claim 83 and wherein the server comprises:

(a) a remote renewable security element;

(b) an entitlement message generator; and

(c) a control word message generator, and

the protected content is broadcast by the head-end, the head-end providing an access criteria reference and a control word for accessing the protected content, and

said entitlement message generator receives the access criteria reference from the head-end and queries said remote renewable security element to determine whether the at least one of the non-security-element recipient modules is entitled to receive the protected content, such that if the at least one of the non-security-element recipient modules is entitled to receive the protected content, said entitlement message generator generates a VEMM comprising an encrypted access key and the access criteria reference, and

if the at least one of the non-security-element recipient modules is entitled to receive the protected content, said control word message generator receives the control word from the head-end and generates a VECM comprising an encrypted control word, such that the at least one of the non-security-element recipient modules cannot access the protected content without said VEMM and said VECM.

Claim 116 (new): The system according to claim 83 and wherein the server comprises:

(a) a remote renewable security element for determining whether the at least one of the non-security-element recipient modules has at least one entitlement to the protected content;

(b) a VEMM generator for generating a first message containing a first key, said VEMM generator only generating said first message if the at least one of the non-security-element recipient modules has said at least one entitlement; and

(c) a VECM generator for generating a second message containing a second key, said second key being encrypted with said first key, wherein the protected content is only accessible according to said second key.

Claim 117 (new): The system according to claim 83 and wherein the renewable security element comprised in each of the first plurality of security-element recipient modules comprises a smart card.